HYDRA — Game Mathematics Document

Version: 4.0 · corresponds to game build v0.88 **Scope:** complete mathematical specification of the HYDRA game family — HYDRA PULL (multiplayer and solo), HYDRA MINORITY (multiplayer and solo), HYDRA BIATHLON and HYDRA HEIST — including commission models, randomness sources, fairness proofs, and accounting invariants. **Audience:** independent test laboratories, aggregators, and operator due-diligence teams.

---

1. FAMILY OVERVIEW

HYDRA is a family of original wagering games — peer-to-peer pool games, honest solo duels and one banked crash title — sharing one wallet, one audit system, and one integration surface. Six game surfaces across four titles are covered by this document:

- **HYDRA PULL — multiplayer**: two opposing pools (BLACK and RED) connected by a spinning wheel; peer-to-peer, the operator is never a counterparty.
- **HYDRA PULL — solo ("Play vs Computer")**: the player against the house with a fixed, disclosed edge from a single BANKRUPT sector.
- **HYDRA MINORITY — multiplayer**: twelve cells, hidden flat-stake bets; the two most-backed cells pay the six least-backed. Strictly peer-to-peer; the outcome is determined by the players' own bets, with randomness used only to break exact ties.
- **HYDRA MINORITY — solo ("the computer's extra cell")**: a 5×5 duel against the house whose entire edge is one extra marked cell, stated openly: RTP 96.00%.
- **HYDRA BIATHLON — solo**: a push-your-luck shooting ladder — call the ring, up to five shots per stake — priced at a flat 96% for every call and **every strategy**; the entire edge is the black outer band of the target.
- **HYDRA HEIST — banked crash, global rounds**: synchronized rounds shared by all players — two animated burglars loot a vault bag by bag, each bag climbing a 30-rung multiplier ladder (×1.05 → ×385.68); cash out before the police arrive. House-banked at a fixed, published **96.00% under the same strategy-invariance law as BIATHLON**.

---

2. HYDRA PULL — MULTIPLAYER MODEL

2.1 State

Each side $s \in \{\text{black}, \text{red}\}$ holds a pool `P_s = S_s + Σ a_i(s)`, where `S_s` is the house seed (display liquidity) and `a_i(s)` are participant position values on side s. Participants are human players and disclosed computer players (§9).

2.2 Round resolution

The wheel of `N` sectors (default 20: percentages {10…100} × both colors) selects sector `(c, p)`. Let the winning side be `W = c`, losing side `L`. The transfer is

```
T = (p / 100) × P_L
```

Every holding on the losing side (seed included) is scaled by `(1 − p/100)`. Every holding on the winning side gains `T × a_i / P_W` — equivalently, all winning holdings scale by the common multiplier `g = 1 + T / P_W`.

2.3 Conservation (zero-sum theorem)

Sum over both sides after resolution:

```
P_L' + P_W' = P_L(1 − p/100) + P_W + (p/100)P_L = P_L + P_W
```

No money is created or destroyed by a spin. This invariant is enforced at runtime to float precision by a continuous audit (§11) and validated by an automated stress test (5,000 randomized events; observed drift $0.0000).

2.4 Commission

Two independent, operator-configurable deductions:

- **Rake** `r ∈ [0, 20]%` — withheld from each transfer: winners share `T(1 − r/100)`; the withheld part accrues to the house ledger.
- **Cash-out fee** `f ∈ [0, 20]%` — deducted at the moment a position converts to wallet balance (voluntary, per-position, and automatic cash-outs alike). All player-facing buttons display **net** amounts.

Return to player. In a peer-pool game RTP is defined against commission only: with `r = f = 0`, aggregate RTP = 100% (strict zero-sum among participants). With commissions active, the aggregate long-run return equals `1 −` (commission actually charged on the player's flows); e.g. `r = 3%` on transfers returns 97% of each transferred amount to the winning side.

2.5 Timing and the lock window

A round is: **betting** (default 10 s) → **spin** (6 s) → **result** (5 s; betting reopens during result). Cash-outs are permitted during result and the **first half** of betting only; bets are accepted until the final instant. Consequence: in the closing seconds money may join the table but cannot leave it, eliminating bait-and-withdraw manipulation (the table observed at lock is the table that plays).

2.6 House seed symmetry

At every betting open the two house seeds are equalized: `S_black = S_red = (S_black + S_red)/2` (an internal zero-sum move). Therefore any pool imbalance is created solely by participants' choices; the house never presents a lopsided pool that a thin-side bet could exploit.

2.7 Exposure bounds

Per spin, a position cannot lose more than `p%` of itself (`p ≤ 100`), and a side cannot pay more than `p%` of its own pool. Operator-set table limits (max bet, max open exposure per player) bound individual exposure; both are broadcast to players in real time.

---

3. HYDRA PULL — SOLO MODEL ("THE HYDRA'S MIRROR")

3.1 Wheel

The standard solo wheel has **21 sectors**: values {10, 20, …, 100} on red and on black (20 sectors) plus one **BANKRUPT** sector. Custom wheels: the player selects `k ∈ [1, 9]` values (each 5–100); the wheel is built as `2k + 1` sectors (both colors + BANKRUPT always present).

3.2 Resolution

Every position plays an independent duel against the house at matched stakes:

- sector `(c, p)`: positions on color `c` gain exactly `+p%`; positions on the other color lose exactly `−p%`;

- BANKRUPT: **all** positions on the table are forfeited to the house.

The house books the net of each spin (`Σ before − Σ after`) in a dedicated Solo P&L account; the global audit (§11) covers it.

3.3 House edge and RTP

For any position, color symmetry of the wheel makes the percentage sectors expectation-neutral; the entire edge is the BANKRUPT sector:

```
E[return per spin] = (2k/(2k+1))·0 + (1/(2k+1))·(−100%) = −100/(2k+1) %
```

Standard wheel (10 value pairs ⇒ 21 sectors): **house edge = 1/21 ≈ 4.7619% of money at risk per spin; RTP = 95.2381%**. Monte-Carlo verification, 10,000,000 simulated spins: measured per-spin return −4.7667%, RTP 95.2333% (within 0.005 pp of theory; convergence ∝ 1/√n).

Custom wheels: edge = `1/(2k+1)`, i.e. from 33.33% (`k=1`, 3 sectors) down to 5.26% (`k=9`, 19 sectors). The wheel composition is always fully visible to the player before betting.

Maximum single-spin outcomes: +100% (a 100% sector for your color) and −100% (BANKRUPT or a 100% sector against you). Because gains and losses are multiplicative per spin, session volatility grows with the number of spins a position rides; there are no hidden multipliers.

3.4 Both-sides play

Holding both colors forms two independent duels; the totals may drift by the difference of the two sides (settled from/to the Solo P&L), never at another player's expense. Both-sides play doubles BANKRUPT exposure and confers no advantage.

---

4. HYDRA MINORITY — MODEL

4.1 Table family and state

One MINORITY room is a **family of flat-stake tables**, one per chip denomination (default $1 / $5 / $10 / $25 / $50 / $100), with one shared wallet and **separate escrows and quorums per table**. The laws of the flat table:

- every bet equals the table's chip — no exceptions (`minBet = maxBetPerCell = chip`);
- **one chip per cell per player** ("one cell — one bet");
- **maximum cells per player = the winner-set size** (6 of 12). Covering more cells would turn the game into riskless harvesting (a player covering the entire quiet side is guaranteed non-negative return); the cap keeps every participant exposed.

Money path per table: `wallet → table escrow (at bet) → wallets (at settle)`. Escrow totals are part of the global conservation identity (§11).

4.2 Round lifecycle

A round is **asynchronous**: it opens, accepts hidden bets, and waits until the **quorum** of distinct players (default 6) is reached. Reaching quorum starts a countdown (default 20 s). Bets are accepted until the countdown expires; **cancels are permitted only before the countdown starts** — the same lock-window law as PULL: in the closing window money may join the table but cannot leave it. During the open and countdown phases only aggregates are public (pot, player count, quorum progress); individual bets remain hidden until the lock.

Players may leave after betting: their bets play without them, and the settlement is stored **on the player's own record** — later rounds at the table can never erase an absent player's result, and open bets and unseen results

survive server restarts (§11).

4.3 Resolution

At lock, the 12 cells are ranked by total money staked on them, descending; exact ties are broken by the pre-committed seed (§7.3), making the ranking fully deterministic and externally verifiable. With cell totals $t_1 \geq t_2 \geq \ldots \geq t_{12}$ after ranking:

- the top **2** cells are the **payers**: every stake on them is lost in full to the pot, $pot = t_1 + t_2$;
- the bottom **6** cells are the **winners**: their stakes $W = t_7 + \ldots + t_{12}$ share the pot pro-rata;
- the middle **4** cells **push**: stakes returned in full.

Every winning stake a is paid $a \times m$ with the common multiplier

$$m = 1 + (pot - rake) / W, \qquad rake = pot \times r/100, \quad r \in [0, 20]$$

so $m \geq 1$: a winner never receives less than the stake back. On the live flat tables, parameters were selected by simulation (12 cells, quorum 6): void rate ≈ 0.4%, action rate (a bet wins or loses rather than pushes) ≈ 60%, median multiplier ≈ ×1.90.

4.4 Conservation theorem

Let S be all stakes in the round: $S = pot + W + Push$. Paid out at settle: winners receive $W \cdot m = W + pot - rake$; pushes receive $Push$. Hence

$$paidOut = W + pot - rake + Push \;\Rightarrow\; S - paidOut - rake = 0$$

Money is conserved exactly; the rake is the only house-bound flow. The engine computes settlements in full IEEE-754 double precision and writes the per-round conservation residual into the journal record (observed $|residual| \leq 10^{-12}$ across randomized 500-round sweeps per engine; module test suite: 21 end-to-end scenarios).

4.5 Void conditions

A round is **void** — all stakes refunded in full — when the winner-side stakes are zero (the quiet six are empty) or no money entered the round. Operator-triggered voids (malfunction handling) refund every stake at face value and are journaled as void records.

4.6 Incentive and manipulation notes

The win condition inverts crowd-following: money added to a cell pushes it **toward** the paying side. Self-targeting is therefore self-defeating — making a cell "heavy" costs exactly the stakes that will be forfeited on it, and making a cell "quiet" requires *not* betting it. Ranking uses **money only** — never player counts, which are a cheap, forgeable signal. Coordinated manipulation requires multi-accounting at stake, which is the operator-level fraud domain (KYC / device controls), not a game-math exposure.

4.7 RTP and commission

MINORITY is strictly zero-sum between players. With $r = 0$, aggregate RTP = 100%; with rake active, aggregate long-run return is $1 - r/100$ of the pot flow (rake applies to the pot only — push returns are never raked).

4.8 Solo mode — the computer's extra cell

The board is **25 cells (5×5)**. Before any bet is accepted, the computer marks **13** cells, committed via the round seed (§7.4). The player marks up to **12** cells; per-cell stakes may differ (chip denominations). At the reveal, a **matched** cell (also held by the computer) loses its stake; an **unmatched** cell pays **1:1**.

House edge. For any single cell, `P(match) = 13/25`, hence

```
E[return per unit staked] = (12/25)·(+1) + (13/25)·(−1) = −1/25 = −4%
```

RTP = 96.00%, identical for every cell and every stake size — the entire edge is the computer's one extra cell (13 vs the player's maximum 12), a single visible object stated in the UI. Monte-Carlo verification: 300,000 simulated full-board rounds, measured RTP 96.02%.

Side bets (available only on a full 12-cell board; resolved from the *same* marking — no additional randomness). Let `M` be the number of matches; `M` follows the hypergeometric distribution `P(M=m) = C(13,m)·C(12,12−m)/C(25,12)`:

Bet	Exact probability	Multiplier	RTP
Exactly 6 match	30.4902%	×3.15	96.04%
4 or fewer match	8.1178%	×11.8	95.79%
3 or fewer match	1.3119%	×73	95.77%

The player cap of 12 (winner-set logic inverted: one below the computer's 13) makes full-board coverage the maximum-action play without ever eliminating exposure.

---

5. HYDRA BIATHLON — MODEL (SOLO)

HYDRA BIATHLON is a solo push-your-luck ladder. One stake loads a clip of up to **5 shots** at a target of 11 concentric scoring zones ringed by a black outer band. Before every shot the player **calls a ring** — "this ring or closer". Landing on the called zone or deeper multiplies the pot; landing below the call — or in the black band — ends the round at zero. The player may cash out between any two shots; five straight hits settle automatically.

5.1 One physical distribution

Every shot draws a single uniform `u ∈ [0,1)` (derivation in §7.5), scored against one fixed cumulative table — the same physics regardless of the call:

Zone	P(land)	P(zone or deeper)
X (heart)	0.64%	0.64%
10	0.96%	1.60%
9	1.60%	3.20%
8	3.20%	6.40%
7	3.20%	9.60%
6	6.40%	16.00%
5	8.00%	24.00%
4	8.00%	32.00%
3	16.00%	48.00%
2	16.00%	64.00%
1	16.00%	80.00%
BLACK (house band)	**20.00%**	—

5.2 The call book

A call on zone `k` wins with the cumulative probability `p_k = P(zone ≥ k)` and multiplies the pot by

```
m_k = 0.96 / p_k        (exactly, for every call)
```

Call	P(win)	Multiplier	Call	P(win)	Multiplier
1+	80.0%	×1.2	7+	9.6%	×10
2+	64.0%	×1.5	8+	6.4%	×15
3+	48.0%	×2	9+	3.2%	×30
4+	32.0%	×3	10	1.6%	×60
5+	24.0%	×4	X	0.64%	×150
6+	16.0%	×6			

The identity `m_k · p_k = 0.96` is displayed in the game and is itself the fairness statement: every call carries the same 96% per-shot return; the calls differ only in volatility.

5.3 The streak refund — one round, one edge

A naive ladder would charge the edge on every shot (riding `k` shots would return `0.96^k`). BIATHLON refunds the compounding: a round settled after `k` consecutive hits pays

```
credited = pot × (1/0.96)^(k−1)
```

— the streak factor is ×1 after one hit, then ×1.0417, ×1.0851, ×1.1303, and ×1.1774 for the full clip. A bust pays zero regardless of streak.

Invariance theorem. Under this book, every fire-or-cash decision node is exactly value-neutral: taking one more shot multiplies the player's expected settled value by `p_k · m_k · (1/0.96) = 1` for every call `k`. By optional stopping, **every strategy — any call sequence, any exit point, adaptive or not — returns exactly 96.00% of the stake per round.** There is no skill-dependent RTP band to certify: RTP is a single number.

Monte-Carlo verification: ride-all-five on call 3+ (150,000 rounds) — measured 95.3%; cash-after-two-hits on call 2+ (200,000 rounds) — 95.8%; both within sampling error of theory (convergence ∝ 1/√n). Settlement arithmetic is exact in double precision (`credited = pot × streak`); rounding is display-only.

5.4 The black band — the family law

The black outer band (20% of shots) beats every call; for the widest call (1+) it is the *only* way to lose. This is the same design law as PULL solo's BANKRUPT sector and MINORITY solo's extra cell: the house's advantage is a single visible object drawn on the playing surface, never a hidden margin in the numbers. Sceneries (WINTER / NIGHT RANGE) are cosmetic layers only and can never alter the geometry, probabilities or payouts.

5.5 Persistence

— THE COMMITTED SEED AND THE ENTIRE LIVE ROUND (STAKE, POT, SHOT LOG) ARE STORED ON THE PLAYER'S PERSISTENT RECORD: A ROUND SURVIVES RECONNECTS AND SERVER RESTARTS, AND THE STAKE OF AN IN-FLIGHT ROUND IS CARRIED AS ESCROW IN THE GLOBAL AUDIT IDENTITY (§11). A DISCONNECT CAN NEVER EAT A STAKE.

— 6. HYDRA HEIST — MODEL (BANKED CRASH, GLOBAL ROUNDS)

HYDRA HEIST is the family's crash-category title: synchronized global rounds in which two animated burglars loot a bank vault bag by bag. Unlike the pool games, HEIST is house-banked — and the entire bank is priced by one law, the same strategy-invariance law as BIATHLON (§5.4): **every cash-out policy returns exactly RTP = 96.00%**.

6.1 Round shape

A round is: **betting window** (default 7 s; each player has two independent bet slots, A and B) → **heist** (bags land one at a time; each landed bag advances the public multiplier one rung) → **police** (round ends; stakes still in play are lost) or **clean getaway** (all 30 bags land; every surviving stake is auto-cashed at the top rung). From bag 1 onward a stake may cash out at any moment for `stake × M_k`, where `k` is the number of bags landed so far.

6.2 The ladder

Per-bag growth accelerates linearly: `g_k = 5% + 1.2 pp × (k − 1)`, and the rung multipliers compound, `M_k = Π_{j≤k} (1 + g_j)`:

k	g_k	M_k	P(reach k)	k	g_k	M_k	P(reach k)
1	5.0%	×1.05	91.43%	16	23.0%	×7.99	12.02%
2	6.2%	×1.12	86.09%	17	24.2%	×9.92	9.68%
3	7.4%	×1.20	80.16%	18	25.4%	×12.44	7.72%
4	8.6%	×1.30	73.81%	19	26.6%	×15.74	6.10%
5	9.8%	×1.43	67.22%	20	27.8%	×20.12	4.77%
6	11.0%	×1.59	60.56%	21	29.0%	×25.96	3.70%
7	12.2%	×1.78	53.98%	22	30.2%	×33.80	2.84%
8	13.4%	×2.02	47.60%	23	31.4%	×44.41	2.16%
9	14.6%	×2.31	41.53%	24	32.6%	×58.88	1.63%
10	15.8%	×2.68	35.87%	25	33.8%	×78.79	1.22%
11	17.0%	×3.13	30.66%	26	35.0%	×106.36	0.90%
12	18.2%	×3.70	25.94%	27	36.2%	×144.87	0.66%
13	19.4%	×4.42	21.72%	28	37.4%	×199.05	0.48%
14	20.6%	×5.33	18.01%	29	38.6%	×275.88	0.35%
15	21.8%	×6.49	14.79%	30	39.8%	×385.68	0.249%

6.3 The outcome law and the invariance theorem

The hidden death count `N` — bags landed before the police arrive — is drawn so that the survival law holds on every rung:

```
P(N ≥ k) = RTP / M_k          for all k = 1…30
```

Concretely, one uniform `u ∈ [0,1)` drives the whole round (derivation in §7.6): `N = max { k : u < RTP / M_k }`, with `N = 0` when `u ≥ RTP / M_1`. The thresholds are nested (`M_k` strictly increasing), so `N` is well-defined and monotone in `u`.

Theorem (strategy invariance). For any fixed cash-out rung `k`: `EV = M_k × P(N ≥ k) = M_k × RTP / M_k = RTP`. Any adaptive or randomized policy is a convex combination of fixed-rung outcomes, so its return is exactly RTP as well. The one-line proof is the entire pricing of the game — there is no other edge anywhere.

Corollaries. Instant police: `P(N = 0) = 1 − 0.96/1.05 = 8.5714%`. Clean getaway: `P(N ≥ 30) = 0.96 / 385.68 = 0.2489%` — one round in ~402 — paid ×385.68. Expected depth: `E[N] = Σ_k 0.96/M_k = 8.04` bags.

6.4 Two slots and the window law

Both slots may be staked in the same window (minimum $1 each; the slots ride and settle independently — the classic two-bet crash pattern: cash one early, let the other run). Bets are accepted **only while the window is open**. A bet sent during a live heist is pre-debited and queued for the next round, cancellable at full refund until that round starts. Mid-round live entry is forbidden by arithmetic, not by taste: conditional on a round having reached rung `j`, `P(N ≥ k | N ≥ j) = M_j / M_k`; a stake entering at rung `j` and cashing at `k` would earn `M_k /`

`M_j` with probability `M_j / M_k` — an exactly 100%-RTP, edge-free product. The pre-debited queue preserves the family law.

6.5 Getaway settlement

If all 30 bags land, every stake not yet cashed is credited `stake × M_30` automatically at settle. The getaway is not a separate random event and adds no house exposure beyond the survival law — it is the same single draw's tail, priced like every other rung (EV = RTP).

6.6 Tempo — a cosmetic law

Bag `k` lands after `max(1700 ms, 5000 / rate(k))` where `rate(k) = min(1.1 + 0.12 (k − 1), 2.9)`: a full 30-bag round fits in ≈68 s. Like BIATHLON's sceneries (§5.4), tempo and all presentation — the animated scenes, the rotating betting-window covers, the periodic cinema intro — are cosmetic only: `N` is fixed at commit time, and no visual event ever touches odds, timing of bets, or payouts.

6.7 Wallet semantics, escrow and restarts

Debit at bet (the stake moves to the round's escrow), credit at cash-out and at settle — two wallet operations per stake. Queued next-round stakes sit in a separate pre-debited pending escrow. Both escrows are terms of the global conservation identity (§11). On process restart, every open and pending HEIST stake is **refunded in full by an automatic sweep** before the first new round opens, journaled as a dedicated event — a restart can never eat a stake or leave a round half-settled. House results are booked per round (`staked − paid`) through the injected-capital door into a dedicated HEIST P&L memo, so banked rounds leave the conservation needle untouched.

6.8 Verification

The automated suites assert, among 54 engine and integration checks: the algebraic identity `EV = 0.96` on all 30 rungs; determinism of `N` from `(seed, round)`; a 200,000-round Monte Carlo — instant police 8.66% observed against 8.57% theoretical, cash-at-1/5/10 strategies within ±1% of 96%, 509 getaways observed against ≈498 expected; a brute-forced getaway round auto-paying ×385.68 to the cent; and money conservation **to the cent** across randomized multi-round sessions including queued bets, cancels, cash-outs and restarts.

---

7. RANDOMNESS AND PROVABLY FAIR

All game outcomes derive from cryptographic primitives (SHA-256, HMAC-SHA-256 over CSPRNG-generated secrets via `crypto.randomBytes`); no linear-congruential or `Math.random` source participates in any outcome.

7.1 PULL multiplayer: pre-committed hash chain

A chain of 100,000 seeds is generated: `s_N = 32 random bytes`, `s_i = SHA256(s_{i+1})`. Rounds consume seeds in ascending order; the **hash of the upcoming seed is always public** (it equals the previously revealed seed). Outcome derivation for round `R` with seed `s`:

```
d = HMAC_SHA256(key = s, msg = SALT ‖ ":" ‖ R)
index = ⌊ (int(d[0:13 hex]) / 2^52) × N_sectors ⌋
```

Verification (performed automatically in the player's browser, and reproducible externally): `SHA256(s) = previous seal` and the index re-derivation. The 52-bit uniform-float method bounds selection bias below `N/2^52 < 5×10⁻¹⁵` — negligible at any laboratory standard. Test overrides (development only) are flagged in the public log and disabled in production. Production note: the salt will be sourced from a public external event (e.g., a future blockchain block hash) after chain commitment, removing any operator freedom in chain selection.

7.2 PULL solo: three-input model

Per player: a server seed (its SHA-256 hash always displayed), a **player-chosen client seed**, and an incrementing nonce:

```
index = ⌊ (int(HMAC_SHA256(serverSeed, clientSeed ‖ ":" ‖ nonce)[0:13]) / 2^52) × N ⌋
```

The player may rotate at any time: the old server seed is revealed for retro-verification of every past spin, and a fresh seed is committed.

7.3 MINORITY multiplayer: per-round commit–reveal tiebreak

MINORITY's outcome needs **no RNG at all**: the players' bets alone determine the ranking. Randomness enters only to break exact money ties, through a per-round commit–reveal:

- at round open, a fresh 32-byte seed is generated and its `SHA-256` hash is **published before any bet is accepted**;
- at lock, the seed itself is revealed. Tiebreak priority for cell `c` in round `R`:

```
prio(c) = int( HMAC_SHA256(seed, R ‖ ":" ‖ c)[0:13 hex] )
```

Equal money ⇒ the higher priority ranks higher. Publishing the seed lets anyone re-derive the complete ordering; the commitment proves the seed predates every bet. The same 52-bit derivation bounds any residual bias below 5×10^{-15}. Open rounds that survive a server restart (§11) are restored **under their original seed and commitment**, so the published hash remains valid.

7.4 MINORITY solo: per-play commit–reveal board

Each player holds a personal committed seed: its SHA-256 is displayed **before** any cells are marked, and the seed is revealed with the result, after which a fresh seed is committed. The computer's 13 cells derive deterministically from the seed via an HMAC-driven Fisher–Yates shuffle over cells 1…25:

```
u_j = int( HMAC_SHA256(seed, R ‖ ":" ‖ j)[0:13 hex] ) / 2^52,   j = 0 … 23
```

successive `u_j` drive the shuffle; the first 13 positions of the shuffled array are the computer's cells. Supplying the revealed seed and this formula regenerates the exact board. The commitment lives on the player's persistent record, so it survives reconnects and server restarts unchanged.

7.5 BIATHLON: per-round commit–reveal shot stream

Each round holds one committed 32-byte seed: its SHA-256 is displayed before the first trigger pull, and the seed is revealed when the round settles (a fresh seed is then committed). Shot `j` (0-based) consumes two nonces — `2j` for the money draw and `2j+1` for the cosmetic impact angle:

```
u_j = int( HMAC_SHA256(seed, R ‖ ":" ‖ 2j)[0:13 hex] ) / 2^52
```

`u_j` is scored against the cumulative table of §5.1. Supplying the revealed seed regenerates every shot of the round; the commitment proves the seed predates the first shot. Because the seed and the live round persist on the player's record, a server restart never breaks a published commitment.

7.6 HEIST: per-round commit–reveal

Each round `R` draws a fresh 32-byte CSPRNG seed. `SHA-256(seed)` is published on the game screen **before the betting window opens**; the seed is revealed with the result. The entire round is a single draw:

```
u = int( first 13 hex chars of HMAC-SHA256(seed, R) ) / 2^52
N = max { k : u < 0.96 / M_k }        (N = 0 if u ≥ 0.96 / M_1)
```

Bag timing carries no randomness — `N` is fully determined at commit time, and the animation merely walks toward it. Supplying the revealed seed regenerates the round; hashing it proves the commitment predates every bet in the window. The same 52-bit derivation bounds residual selection bias below 5×10^{-15}.

---

8. RANDOMNESS QUALITY

Outcome entropy originates from the operating system CSPRNG (`crypto.randomBytes`), and all derivations are keyed SHA-256 constructions. For laboratory evaluation the derivation functions are stateless and reproducible: supplying the revealed seeds and the formulas in §7 regenerates the full outcome sequence, enabling standard statistical batteries (chi-square uniformity over sector indices, serial correlation) to be run directly on production logs (§10).

---

9. COMPUTER PLAYERS AND LIQUIDITY POLICY

9.1 PULL: disclosed symmetric liquidity

During quiet periods, PULL seats may be filled by computer players funded by the house. Their governing laws:

1. **Never responsive:** they do not react to any human action; while humans are present they place bets only in self-contained pairs (one leg per side, seconds apart).
2. **Symmetry at every lock:** at the instant the wheel locks, computer-player money satisfies `B_black = B_red` to the cent (enforced by an exact settle step).
3. Excluded from leaderboards; masked like all players; their wins and losses are the house's own money.

House-safety lemma. With bot money symmetric (`x` per side) on a table with side totals `T_b ≥ T_r`, the expected house result per spin over the color-symmetric wheel is

```
E = (p·x/2)·(T_b/T_r + T_r/T_b − 2) ≥ 0
```

with equality iff `T_b = T_r` (AM–GM). Symmetric liquidity is therefore risk-free on a balanced table and non-negative-EV on an unbalanced one; the house never takes voluntary directional exposure.

9.2 MINORITY: demo greeters only — no bots in real money

In the **public play-money demo**, tables are kept warm by house-funded greeter bots: they join a table **only after a human has bet** (never an empty table), top the table up toward quorum, and stop the moment quorum is met. Their stakes are house play-money, fully reported to the audit ledger (§11) so bot rounds leave the conservation needle untouched.

The **real-money design uses no bots and no simulated players of any kind** — PULL's symmetry lemma has no analogue in a ranked 12-cell game, so the honest answer is abstinence. Real-money liquidity is provided structurally: asynchronous quorum rounds (bets wait; players need not be simultaneous) and network-shared tables (players from every operator site sit at the same global tables).

10. AUDIT JOURNAL

Every round of **every game** appends one line to an **append-only, hash-chained journal** (`h_i = SHA256(h_{i−1} ‖ body_i)`): timestamp, outcome, fairness seed, pools or cell totals, transfer or pot/multiplier, every monetary event (masked identity + token prefix; bot flag), the per-round conservation residual (MINORITY), and the live audit drift. Any retroactive edit breaks the chain. Void/refund actions are themselves journal entries. HEIST rounds journal the revealed seed, bag count, end reason and the round's staked/paid totals (empty rounds keep the show running but stay out of the journal); the restart refund sweep (§6.7) is itself a journaled event. Round and transaction CSV exports are generated directly from the chain. Monthly archives preserve cross-file integrity.

11. ACCOUNTING INVARIANTS

- All internal monetary arithmetic is IEEE-754 double precision; **rounding is display-only**.
- Global identity, checked continuously: `seeds + house ledgers + wallets + all positions + MINORITY table escrows + live BIATHLON round stakes + HEIST open-round stakes + HEIST next-round queue + bot bankrolls = injected capital` ; the difference ("drift") is displayed in the back office and recorded in the journal, with **phase-level attribution**: every check is tagged with the game phase that ran last, so any movement names its source. Observed value across the automated test suites (14 PULL end-to-end scenarios; 21 MINORITY end-to-end scenarios; randomized conservation sweeps): **$0.0000** (residuals ≤ 10^{-12}).
- Greeter-bot money entering or leaving MINORITY escrow is reported to the injected-capital ledger at bet and settle time, keeping the audit flat across bot-assisted demo rounds.
- Solo play (PULL solo, MINORITY solo and BIATHLON alike) books the house net through the same injected-capital door into a dedicated solo P&L memo — solo rounds leave the conservation needle untouched. HEIST, the banked global-rounds title, books each round's `staked − paid` through the identical door into its own P&L memo.
- **Persistence:** wallets, PULL positions, MINORITY open bets (with their seeds and commitments), BIATHLON live rounds (seed, stake and shot log) and each player's latest unseen settlement survive server restarts; "open positions are never lost" holds across the family. HEIST states its restart law differently but just as strictly: open and queued stakes are **refunded in full** by an automatic journaled sweep (§6.7) — never eaten, never half-settled.
- Malfunction clause (player rules §8): voided rounds return stakes; the operation is ledger-neutral by construction (§10).

12. SUMMARY OF CONFIGURABLE PARAMETERS

HYDRA PULL

Parameter	Range	Default
Betting / spin / result duration	5–120 s / fixed / fixed	10 / 6 / 5 s
Rake on transfers	0–20%	0
Cash-out fee	0–20%	0
Max bet / max open exposure	0 = off	off
Computer players: count / bet range	0–30 / $1–2,000	8 / $50–500
Solo custom wheel values	1–9 values, 5–100%	standard 21-sector

HYDRA MINORITY

Parameter	Range	Default
Chip tables	operator-configurable set	$1 / $5 / $10 / $25 / $50 / $100
Cells / winners / payers	fixed by game design	12 / 6 / 2
Quorum (distinct players)	2–20	6
Countdown after quorum	5–60 s	20 s
Reveal duration	1–15 s	4 s
Rake on the pot	0–20%	0
Demo greeter bots	on / off (demo builds only)	on

HYDRA MINORITY — solo mode

Parameter	Range	Default
Board / computer cells / player cap	fixed by game design	25 / 13 / 12
Chip denominations (per-cell stakes may differ)	operator-configurable set	$1 / $5 / $10 / $25 / $50 / $100
Side bets	on full board only	×3.15 / ×11.8 / ×73 (fixed book)

HYDRA BIATHLON

Parameter	Range	Default
Stake	any amount ≥ minimum, cent precision	min $1; chips $1–$100 as shortcuts
Shots per round	fixed by game design	5
Call book	fixed: `m = 0.96 / p`	×1.2 … ×150
Streak refund	fixed: `(1/0.96)^(k−1)`	full clip ×1.1774
Sceneries	cosmetic only — never touch the odds	WINTER / NIGHT RANGE

HYDRA HEIST

Parameter	Range	Default
Betting window	3–30 s	7 s
Bet slots per player	fixed by game design	2 (A and B), independent
Ladder	fixed: `g_k = 5% + 1.2pp×(k−1)`, 30 rungs	×1.05 → ×385.68
RTP	fixed by the family law	96.00% — every strategy
Stake	any amount ≥ minimum, cent precision	min $1; chips $1–$100 as shortcuts
Intermission (police / getaway)	1–30 s	5.5 s / 9 s
Bag tempo	fixed cosmetic curve (§6.6)	5.0 s → 1.7 s per bag
Covers & cinema intro	cosmetic only — never touch the odds	rotating covers · intro each session + every 15th round

Prepared by the HYDRA development team. Reproduction formulas in §2–§7 are sufficient to independently regenerate and verify all game outcomes and payouts from published data. Contact: ilia@hydrapull.com · hydrapull.com